SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Petar Dević

KONAČNODIMENZIONALNE ALGEBRE S DIJELJENJEM

Diplomski rad

Voditelj rada:
Doc. dr. sc. Ilja Gogić

Zagreb, 2019.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Ovaj rad posvećen je mojoj obitelj i prijateljima koji su bili uz mene spremni pomoći kad god je bilo potrebno te pokojnoj baki koja nije dala da me otpuše vjetar.

Velike zahvale mentoru doc. dr. sc. Ilji Gogiću, prije svega na razumijevanju i strpljenju, ali i korisnim savjetima udjeljenim pri izradi ovog rada.

Sadržaj

Uvod

Konačnodimenzionalne algebre s dijeljenjem predstavljaju jednu od najstarijih tema u nekomutativnoj algebri. Same začetke nekomutativne teorije postavio je W. H. Hamilton 1843. godine "otkrićem" kvaterniona, odnosno 4-dimenzionalne realne algebre s dijeljenjem. Kasnije su, nezavisno jedan od drugoga, matematičari F. G. Frobenius (1878.godine) i C. S. Peirce (1881.godine) pokazali da su upravo realni brojevi, kompleksni brojevi te kvaternioni jedini primjeri realnih konačnodimenzionalnih asocijativnih algebri s dijeljenjem. Taj rezultat je danas u literaturi poznat kao Frobeniusov teorem.

U prvom dijelu rada, fokus stavljamo na polaganu izgradnju teorije koja će nas dovesti do prvog bitnijeg teorema obrađenog u radu, a to je upravo Frobeniusov teorem za konačnodimenzionalne realne algebre s dijeljenjem.

Nakon što dokažemo Frobeniusov teorem, nastavljamo s daljnjom izgradnjom teorije u svrhu otkrivanja strukture konačnodimenzionalnih algebri. Od posebnog interesa su nam strukturalni teoremi škotskog matematičara J. H. M. Wedderburna koji je 1907. godine objavio rad u kojem je dokazao da je svaka konačnodimenzionalna poluprosta algebra direktni produkt matričnih algebri nad algebrama s dijeljenjem. Razne verzije rezultata ovog rada dostupne su u mnogim sveučilišnim matematičkim udžbenicima te su bazirane na konceptima modula nad algebrama. Ipak, u ovom diplomskom radu bazirali smo se na pristup slovenskog matematičara M. Brešara koji je zbog upotrebe vrlo bazičnog matematičkog alata svakako mnogo pristupačniji. Zbog toga bi tematika ovog rada, koja se standardno predaje na poslijediplomskim studijima, mogla bi biti prihvatljiva i studentima preddiplomskih i diplomskih studija.

Oznake

$\mathbb{N}$	Prirodni brojevi
$\mathbb{Z}$	Cijeli brojevi
$\mathbb{R}$	Realni brojevi
$\mathbb{C}$	Kompleksni brojevi
$\mathbb{H}$	Kvaternioni
$\mathbb{O}$	Oktonioni
F	Fiksirano polje
$Z(R)$	Centar prstena R
$M(A)$	Multiplikacijska algebra od algebre A
$M_n(R)$	Prsten svih n $\times$ n matrica nad R
$T_n(F)$	Algebra gornje trokutastih n $\times$ n matrica nad F
$R \cong R'$	Izomorfni prsteni ili algebre
$\ker \phi$	Jezgra homomorfizma ϕ
$\operatorname{im} \phi$	Slika homomorfizma ϕ
$\operatorname{End}_F(V)$	Algebra linearnih operatora vektorskog prostora V nad F
$V_1 \oplus \cdots \oplus V_n$	Direktna suma konačne familije vektorskih prostora ili Abelovih grupa
$R_1 \times \cdots \times R_n$	Direktni produkt konačne familije prstena ili algebri
E_{ij}	Standardne matrične jedinice u matričnom prstenu $M_n(R)$
e_{ij}	Matrične jedinice
$I + J$	Zbroj ideala
IJ	Produkt ideala
$R[\omega]$	Prsten/algebra polinoma nad R u jednoj varijabli
$\dim_F V$	Dimenzija vektorskog prostora V nad poljem F
$[A : F]$	Dimenzija algebre A nad poljem F

Poglavlje 1

Osnovni pojmovi i tvrdnje

Za početak definirajmo neke od pojmova koje ćemo koristiti u ovom diplomskom radu.

Alegbre

U ovom radu promatramo samo asocijativne algebre. Dakle, **algebra** A nad poljem F, ili F-**algebra** je vektorski prostor nad poljem F na kojem je zadana operacija **množenja**, tj. asocijativna binarna operacija $A \times A \to A, (a, b) \mapsto ab$ koja je bihomogena s obzirom na operaciju množenja skalarom i distributivna slijeva i zdesna s obzirom na operaciju zbrajanja na A. Drugim riječima vrijedi:

$$a(bc) = (ab)c, \quad \lambda(ab) = (\lambda a)b = a(\lambda b), \quad a(b + c) = ab + ac,$$

$$(a + b)c = ac + bc, \quad \text{za sve } a, b, c \in A \text{ i } \lambda \in F.$$

Ako vrijedi $ab = ba$ za sve $a, b \in A$ onda kažemo da je A **komutativna algebra**.

Jedinica u algebri A je element $1 \in A$ takav da je

$$1a = a1 = a \quad \text{za sve } a \in A.$$

Ako jedinica postoji, lako možemo provjeriti da je ona jedinstvena. **Unitalna algebra** je algebra u kojoj postoji jedinica.

Ako je A unitalna algebra, tada za element $a \in A$ kažemo da je **invertibilan** ako postoji element a^{-1} takav da je

$$a^{-1}a = aa^{-1} = 1.$$

Element a^{-1}, ako postoji, je jedinstven i nazivamo ga **inverz** od a.

Podskup B algebre A zove se **podalgebra** od A ako je B algebra s obzirom na operacije koje su definirane kao restrikcije operacija algebre A.

Za podalgebru B unitalne algebre A kažemo da je **unitalna podalgebra**, ako B sadrži jedinicu algebre A. Napomenimo da je moguće da je B unitalna algebra, ali da B nije unitalna podalgebra od A. Naime, moguće je da B ima jedinicu, ali da ta jedinica nije jednaka jedinici algebre A. Ako je A unitalna algebra, za $\lambda \in F$, element $\lambda 1 \in A$ zapisivat ćemo jednostavno kao λ. Nadalje, u tom slučaju F identificiramo s $F1$ te na taj način smatramo da je F unitalna podalgebra od A.

Neka su A i B algebre. Za preslikavanje $\phi : A \to B$ kažemo da je **homomorfizam algebri** ako je ϕ linearno i multiplikativno, tj.

$$\phi(\lambda a + \mu b) = \lambda\phi(a) + \mu\phi(b) \quad \text{i} \quad \phi(ab) = \phi(a)\phi(b)$$
$$\text{za svaki } \lambda, \mu \in F \text{ i } a, b \in A.$$

Ako su A i B unitalne algebre s jedinicama 1_A i 1_B i ako vrijedi $\phi(1_A) = 1_B$ onda se ϕ zove **unitalni homomorfizam**. Injektivni homomorfizam zove se **monomorfizam**, surjektivni **epimorfizam**, a bijektivni **izomorfizam**. Za algebre A i B kažemo da su **izomorfne** ako postoji izomorfizam $\phi : A \to B$.

Budući da su algebre ujedno i prsteni, razne pojmove vezane uz prstene ima smisla promatrati i za algebre, uz neke male preinake. Na primjer, **podalgebra** je potprsten koji je ujedno i potprostor. Slično, **ideali algebre**, su ideali u istom smislu kao i ideali prstena, ali su ujedno i vektorski potprostori.

S obzirom na to da su nam od posebnog interesa u ovom radu konačnodimenzionalne algebre, navedimo još i što smatramo pod konačnodimenzionalnom algebrom. Kažemo da je A **konačnodimenzionalna algebra** ako je A konačnodimenzionalna kao vektorski prostor. Dimenziju A nad F označavat ćemo s

$$[A : F].$$

Ako je R prsten ili algebra, tada skup

$$Z(R) := \{c \in R \mid cx = xc \text{ za sve } x \in R\}$$

nazivamo **centar** od R, a njegove elemente nazivamo **centralnim elementima.**

Algebra polinoma

Neka je R proizvoljni prsten. Definiramo **polinom** nad R kao beskonačnu sumu

$$\sum_{i=0}^{\infty} a_i \omega^i = a_0 + a_1\omega + a_2\omega^2 + \ldots,$$

gdje je $a_i \in R$ i konačno mnogo a_i je različito od 0. Elementi a_i nazivaju se **koeficijenti**. Koeficijent a_0 naziva se **slobodni član**. Ako je $n \geq 0$ takav da $a_i = 0$ za sve $i > n$ i $a_n \neq 0$, onda prethodni polinom obično pišemo kao

$$f(\omega) = a_0 + a_1\omega + \ldots + a_n\omega^n.$$

Za ovaj polinom kažemo da je **stupnja** n te a_n nazivamo njegovim **vodećim koeficijentom**. Ako je $a_i = 0$ za sve $i \geq 0$, onda odgovarajući polinom označavamo s 0. Polinom koji je ili 0 ili stupnja 0 nazivamo **konstantni polinom**.

Zbrajanje i množenje dvaju polinoma definiramo sa

$$\sum_{n=0}^{\infty} a_n\omega^n + \sum_{n=0}^{\infty} b_n\omega^n := \sum_{n=0}^{\infty}(a_n + b_n)\omega^n,$$

$$\left(\sum_{n=0}^{\infty} a_n\omega^n\right)\left(\sum_{n=0}^{\infty} b_n\omega^n\right) := \sum_{n=0}^{\infty} c_n\omega^n, \quad \text{gdje je } c_n = \sum_{n=0}^{\infty} a_i b_{n-i}.$$

Uz ove operacije skup svih polinoma nad R je prsten koji označavamo s $R[\omega]$ i nazivamo **prsten polinoma** (u jednoj varijabli). U ovom radu nas primarno zanima situacija kada je $R = F$ polje.

Dodatno, ako je A algebra, tada $A[\omega]$ postaje algebra uz operaciju množenja skalarom

$$\lambda\left(\sum_{n=0}^{\infty} a_i\omega^n\right) := \sum_{n=0}^{\infty}(\lambda a_n)\omega^n.$$

Algebarska zatvorenost

Definicija 1.0.1. *Polje F je **algebarski zatvoreno** ako svaki nekonstantni polinom u $F[\omega]$ ima korijen u F.*

Napomena 1.0.2. *Ako je F algebarski zatvoreno, onda se svaki polinom $f(\omega) \in F[\omega]$ stupnja $n \geq 1$ može faktorizirati u obliku*

$$f(\omega) = c(\omega - a_1)\cdots(\omega - a_n),$$

za neke $c, a_1, \ldots, a_n \in F$.

Primjer 1.0.3. *Osnovni primjer algebarski zatvorenog polja je polje kompleksnih brojeva $\mathbb{C}$. S druge strane, polje realnih brojeva $\mathbb{R}$ nije algebarski zatvoreno jer npr. polinom $f(\omega) = \omega^2 + 1$ nema korijen u $\mathbb{R}$.*

Matrične algebre

Skup svih realnih $n \times n$ matrica, $M_n(\mathbb{R})$ je prsten (odnosno algebra) uz standardne operacija na matrica. Za $n \geq 2$ ovaj prsten nije komutativan. Ulogu od $\mathbb{R}$ u $M_n(\mathbb{R})$ možemo zamijeniti drugim poljima, ali i prstenima odnosno algebrama. Uzmimo proizvoljni prsten R i $n \in \mathbb{N}$. Za svaki $a_{ij} \in R, 1 \leq i, j \leq n$, s (a_{ij}) označavamo $n \times n$ matricu

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}.$$

Skup svih $n \times n$ matrica nad R označavamo s $M_n(R)$. Na $M_n(R)$ definiramo operacije zbrajanja i množenja na sljedeći način

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij})$$

i

$$(a_{ij})(b_{ij}) := (c_{ij}), \quad \text{gdje je } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Uz te operacije $M_n(R)$ postaje prsten. Ako R ima jedinicu, tada i $M_n(R)$ ima jedinicu (jedinična matrica).

Nadalje, ako je $R = A$ algebra, onda $M_n(A)$ postaje algebra, uz prethodno definirane operacije i operaciju množenja skalarom

$$\lambda(a_{ij}) := (\lambda a_{ij}).$$

Standardne matrične jedinice

Definicija 1.0.4. *Neka je $M_n(S)$ matrični prsten, gdje je S proizvoljan unitalni prsten. Neka je E_{ij} matrica čiji je element na (i, j) mjestu 1, a svi ostali elementi te matrice su 0. E_{ij}, $1 \leq i, j \leq n$ nazivamo **standardnim matričnim jedinicama**. Za $a \in S$ koristimo oznaku aE_{ij} kojom označavamo matrice čiji je element na mjestu (i, j) $a \in S$, a ostali elementi su 0. Svaka matrica $M_n(S)$ je suma takvih matrica. Primijetimo da za svaki $A = (a_{ij}) \in M_n(S)$ imamo*

$$E_{ij} A E_{kl} = a_{jk} E_{il} \text{ za sve } 1 \leq i, j, k \leq n. \tag{1.1}$$

Poglavlje 2

Konačnodimenzionalne algebre s dijeljenjem

Definicija 2.0.1. *Unitalni prsten R je **prsten s dijeljenjem**, ako je svaki ne-nul element u R invertibilan.*

*Analogno definiramo pojam **algebre s dijeljenjem**. Algebru s dijeljenjem u ovom radu obično ćemo označavati s D.*

2.1 Frobeniusov teorem

Krenimo s iskazom i dokazom pomoćnih tvrdnji koje će nas dovesti do odgovora na pitanja postavljena u uvodnom dijelu rada.

Ako drugačije nije istaknuto, tijekom čitavog ovog odjeljka pretpostavljamo da je D realna algebra s dijeljenjem konačne dimenzije n.

Lema 2.1.1. *Za svaki $x \in D$ postoji $\lambda \in \mathbb{R}$ takav da je $x^2 + \lambda x \in \mathbb{R}$.*

Dokaz. Za proizvoljan $x \in D$ promotrimo elemente

$$1, x, x^2, x^3, \ldots, x^n.$$

Budući da je D n-dimenzionalna, ti elementi su sigurno linearno zavisni. Dakle, postoje skalari $\alpha_0, \ldots, \alpha_n \in \mathbb{R}$ koji nisu svi nula tako da vrijedi

$$\sum_{i=0}^{n} \alpha_i x^i = 0.$$

Definirajmo polinom $f(\omega) \in \mathbb{R}[\omega]$ s

$$f(\omega) := \sum_{i=0}^{n} \alpha_i \omega^i.$$

Tada je $f(\omega)$ stupnja najviše n i vrijedi $f(x) = 0$. Iz fundamentalnog teorema o algebri slijedi da polinom $f(\omega)$ možemo faktorizirati na linearne i kvadratne faktore u $\mathbb{R}[\omega]$. Dakle, imamo

$$f(\omega) = (\omega - \beta_1) \cdots (\omega - \beta_r)(\omega^2 + \lambda_1\omega + \mu_1) \cdots (\omega^2 + \lambda_s\omega + \mu_s),$$

za neke $\beta_i, \lambda_i, \mu_i \in \mathbb{R}$. S obzirom na to da je $f(x) = 0$, vrijedi

$$(x - \beta_1) \cdots (x - \beta_r)(x^2 + \lambda_1 x + \mu_1) \cdots (x^2 + \lambda_s x + \mu_s) = 0.$$

Kako je D algebra s dijeljenjem, ona sigurno nema djelitelja nule pa jedan od gornjih faktora mora biti jednak 0. Dakle, x je korijen linearnog ili kvadratnog polinoma u $\mathbb{R}[\omega]$ te slijedi željeni zaključak. □

Motivirani činjenicom da jednodimenzionalni potprostor $\mathbb{R}i$ od $\mathbb{C}$ možemo opisati kao skup svih $z \in \mathbb{C}$ takvih da je z^2 nepozitivan realni broj, za konačnodimenzionalnu realnu algebru s dijeljenjem definiramo sljedeći skup:

$$V := \{v \in D \mid v^2 \in \mathbb{R},\ v^2 \leq 0\}.$$

Napomena 2.1.2. *Primijetimo da ako je $x \in D \setminus V$ takav da je $x^2 \in \mathbb{R}$, onda je $x^2 > 0$ pa stoga vrijedi $x^2 = \alpha^2$ za neki $\alpha \in \mathbb{R}$. Dakle, $(x - \alpha)(x + \alpha) = 0$ iz čega je $x = \pm\alpha \in \mathbb{R}$.*

Lema 2.1.3. *Skup V je linearni potprostor od D. Nadalje, $D = \mathbb{R} \oplus V$.*

Dokaz. Za početak jasno je da vrijedi $\mathbb{R} \cap V = \{0\}$ te da je V zatvoren na množenje skalarom. Pokažimo da je $u + v \in V$ ako su $u, v \in V$. Pretpostavimo da su u, v linearno nezavisni. Tvrdimo da je $\{1, u, v\}$ linearno nezavisan skup. Uzmemo li $\alpha, \beta, \gamma \in \mathbb{R}$ takve da vrijedi $\alpha u = \beta v + \gamma 1$, kvadriranjem obje strane slijedi da je $\beta\gamma v \in \mathbb{R}$, stoga $\beta = 0$ ili $\gamma = 0$ iz čega slijedi da je $\alpha = \beta = \gamma = 0$. Dakle, skup $\{1, u, v\}$ je linearno nezavisan.

Kako su $u, v \in D$ iz leme 2.1.1 slijedi da za svaki $u + v \in D$ postoje $\lambda, \mu \in \mathbb{R}$ takvi da:

$$(u + v)^2 + \lambda(u + v) \in \mathbb{R},$$
$$(u - v)^2 + \mu(u - v) \in \mathbb{R}.$$

Promotrimo li zbroj kvadratnih članova, vidimo da:

$$(u + v)^2 + (u - v)^2 = 2u^2 + 2v^2 \in \mathbb{R} \text{ za } u, v \in V.$$

Dakle, za zbroj linearnih članova mora vrijediti: $\lambda(u + v) + \mu(u - v) \in \mathbb{R}$, što možemo zapisati kao

$$s := (\lambda + \mu)u + (\lambda - \mu)v \in \mathbb{R}.$$

Tada je

$$(-s)1 + (\lambda + \mu)u + (\lambda - \mu)v = 0.$$

Kako je $\{1, u, v\}$ linearno nezavisan skup zaključujemo da $\lambda + \mu = \lambda - \mu = 0$, odnosno $\lambda = \mu = 0$. Stoga je $(u + v)^2 \in \mathbb{R}$.

Pretpostavimo da $u + v \in D \setminus V$, odnosno $(u + v)^2 > 0$. Iz napomene 2.1.2 vidimo da je $u + v \in \mathbb{R}$. Neka je stoga $r \in \mathbb{R}$ takav da je $u + v = r$. Tada je

$$0 = (-r)1 + u + v,$$

što je u kontradikciji s činjenicom da je $\{1, u, v\}$ linearno nezavisan skup.

Dakle, $(u + v)^2 \in \mathbb{R} \wedge (u + v)^2 \leq 0 \Rightarrow u + v \in V$, iz čega slijedi željeni zaključak da je $V \leq D$.

Pokažimo još da je $D = \mathbb{R} \oplus V$. Kako je $\mathbb{R} \cap V = \{0\}$, dovoljno je pokazati da je $D \setminus \mathbb{R} \subseteq \mathbb{R} + V$, odnosno da se svaki element iz $D \setminus \mathbb{R}$ može prikazati kao zbroj jednog elementa iz $\mathbb{R}$ i jednog elementa iz V. Neka je $x \in D \setminus \mathbb{R}$. Prema lemi 2.1.1 postoji $\lambda \in \mathbb{R}$ takav da je $s := x^2 + \lambda x \in \mathbb{R}$. Kako je

$$s = x^2 + \lambda x = \left(x + \frac{\lambda}{2}\right)^2 - \frac{\lambda^2}{4},$$

slijedi

$$\left(x + \frac{\lambda}{2}\right)^2 = s + \frac{\lambda^2}{4} \in \mathbb{R}.$$

Odavde vidimo da mora vrijediti $x + \frac{\lambda}{2} \in V$ ili $(x + \frac{\lambda}{2})^2 > 0$. Pretpostavimo da je $(x + \frac{\lambda}{2})^2 > 0$. Iz napomene 2.1.2 vidimo da je $r := x + \frac{\lambda}{2} \in \mathbb{R}$. Tada je $x = r - \frac{\lambda}{2} \in \mathbb{R}$, što je u kontradikciji s početnom pretpostavkom da je $x \in D \setminus \mathbb{R}$. Dakle $x + \frac{\lambda}{2} \in V$ i prema tome

$$x = -\frac{\lambda}{2} + \left(x + \frac{\lambda}{2}\right) \in \mathbb{R} + V.$$

□

Definicija 2.1.4. *Za sve $u, v \in V$ definiramo*

$$u \circ v := uv + vu.$$

Napomena 2.1.5. *S obzirom na to da je za $u, v \in V$,*

$$u \circ v = (u + v)^2 - u^2 - v^2,$$

iz leme 2.1.3 slijedi da je $u \circ v \in \mathbb{R}$.

Lema 2.1.6. *Ako je $n > 2$, tada postoje $i, j, k \in D$ takvi da je*

$$i^2 = j^2 = k^2 = -1, \tag{2.1}$$

$$ij = -ji = k,\ ki = -ik = j,\ jk = -kj = i, \tag{2.2}$$

te je $\{1, i, j, k\}$ linearno nezavisan skup.

Dokaz. Iz leme 2.1.3 vidimo da V ima dimenziju $n - 1 > 1$. Stoga možemo odabrati linearno nezavisne $v, w \in V$. Neka je

$$u := w - \frac{w \circ v}{v \circ v} v.$$

Primijetimo da je $u \neq 0$ i $u \circ v = 0$. Iz (2.1) vidimo da možemo definirati i i j na sljedeći način:

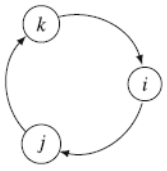
$$i := \frac{1}{\sqrt{-u^2}} u, \quad j := \frac{1}{\sqrt{-v^2}} v, \quad k := ij.$$

Lako je provjeriti da (2.1) i (2.2) vrijede pa iz njih dobivamo da je

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = {\alpha_0}^2 + {\alpha_1}^2 + {\alpha_2}^2 + {\alpha_3}^2 \tag{2.3}$$

pozitivan realan broj za sve $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ koji nisu istovremeno nula. Stoga, slijedi da su $1, i, j, k$ linearno nezavisni. □

Formule iz (2.1) i (2.2) lako možemo pamtiti pomoću sljedećeg dijagrama: Idemo li u



smjeru kazaljke na satu, produkt dva uzastopna elementa je treći, a ako idemo u suprotnom smjeru od kazaljke na satu, produkt dva uzastopna elementa daje negativan treći element.

Korolar 2.1.7. *Ne postoji* 3*-dimenzionalna realna algebra s dijeljenjem.*

Dokaz. Prema lemi 2.1.6, za $n > 2$ D sadrži 4 linearno nezavisna elementa $1, i, j, k$. Dakle $n > 3$. □

Definicija 2.1.8. *Ako je* $n = 4$, $\{1, i, j, k\}$ *je baza od* D *uz množenje definirano u (2.1) i (2.2).* ***Konjugiranu vrijednost*** *nekog* $h = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in D$ *definiramo kao:*

$$\overline{h} := \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k.$$

Korolar 2.1.9. *Ako je* $n = 4$*, tada je* D *algebra s dijeljenjem. Štoviše,* D *je do na izomorfizam jedinstvena realna* 4*-dimenzionalna algebra s dijeljenjem.*

Dokaz. Ako je $h \in D$, $h \neq 0$, onda iz (2.3) slijedi da je $h\overline{h} = \overline{h}h$ nenegativan skalar. Stoga svaki nenul element $h \in D$ ima inverz

$$h^{-1} = \frac{1}{h\overline{h}}\overline{h}.$$

Prema tome, D je algebra s dijeljenjem.

Sada pretpostavimo da je D' neka druga 4-dimenzionalna algebra s dijeljenjem s pripadnim elementima $1', i', j', k'$ koji zadovoljavaju analogne relacije (2.1) i (2.2). Tada se lako provjeri da je preslikavanje $\phi : D \to D'$ definirano s

$$\phi(\alpha_0 1 + \alpha_1 i + \alpha_2 j + \alpha_3 k) := \alpha_0 1' + \alpha_1 i' + \alpha_2 j' + \alpha_3 k'$$

izomorfizam algebri. □

Standardna oznaka za ovu 4-dimenzionalnu nekomutativnu realnu algebru s dijeljenjem (koje je prema korolaru 2.1.9 jedinstvena do na izomorfizam) je $\mathbb{H}$, u čast irskom matematičaru W. R. Hamiltonu, koju je 1843. godine osmislio tijekom šetnje Dublinom. Elementi algebre $\mathbb{H}$ nazivaju se **kvaternioni**. Čitava priča oko nastanka kvaterniona dokumentirana je u Hamiltonovim pismima te je samu formulu $i^2 = j^2 = k^2 = ijk = -1$ moguće pronaći ugraviranu na mostu u Dublinu pod imenom "Broom bridge", kraj kojeg se Hamilton i dosjetio spomenute formule.

Teorem 2.1.10 (Frobenius)**.** *Konačnodimenzionalna realna algebra s dijeljenjem D je izomorfna s $\mathbb{R}$, $\mathbb{C}$ ili $\mathbb{H}$.*

Dokaz. Ako je $n = 1$, onda je $D \cong \mathbb{R}$. Ako je $n = 2$, onda je prema lemi 2.1.3 $\dim V = 1$ (jer je $\dim D = \dim \mathbb{R} + \dim V = 2$). Stoga, D sadrži element i takav da je $i^2 = -1$ pa je onda $D \cong \mathbb{C}$. Iz korolara 2.1.7 vidimo da $n \neq 3$. Ako je $n = 4$ onda je $D \cong \mathbb{H}$.

Pretpostavimo da je $n > 4$ i neka su i, j, k elementi iz leme 2.1.6. Kako je dimenzija od V jednaka $n - 1$, postoji $v \in V$ koji ne leži u linearnoj ljusci elemenata i, j, k. Stoga je

$$e := v + \frac{i \circ v}{2} i + \frac{j \circ v}{2} j + \frac{k \circ v}{2} k$$

nenul element u V. Zaista, ako bi bilo $e = 0$, onda

$$v = -\frac{i \circ v}{2} i - \frac{j \circ v}{2} j - \frac{k \circ v}{2} k.$$

Kako su $\frac{i \circ v}{2}, \frac{j \circ v}{2}, \frac{k \circ v}{2} \in \mathbb{R}$, to je u kontradikciji s pretpostavkom da v ne leži u linearnoj ljusci elemenata i, j, k. Lako se provjeri da takav element $e \in V$ zadovoljava jednakosti

$$i \circ e = j \circ e = k \circ e = 0. \tag{2.4}$$

Pokažimo npr. $i \circ e = 0$. Stavimo $c_1 := \frac{i \circ v}{2}$, $c_2 := \frac{j \circ v}{2}$, $c_3 := \frac{k \circ v}{2} \in \mathbb{R}$. Tada je

$$\begin{aligned} i \circ e &= i \circ v + i \circ (c_1 \cdot i) + i \circ (c_2 \cdot j) + i \circ (c_3 \cdot k) \\ &= i \circ v + c_1 \cdot (i \circ i) + c_2 \cdot (i \circ j) + c_3 \cdot (i \circ k) \\ &= i \circ v - 2 \cdot c_1 \\ &= iv + vi - 2 \cdot \left(\frac{iv}{2} + \frac{vi}{2} \right) \\ &= 0. \end{aligned}$$

Stoga, iz prva dva identiteta u (2.4) zaključujemo $eij = -iej = ije$, ali iz trećeg identiteta dobivamo kontradikciju s obzirom na to da je $ij = k$. Stoga, n može biti samo 1,2 ili 4. □

Dokazom klasifikacijskog Frobeniusovog teorema dokazali smo da (do na izomorfizam) postoje točno tri konačnodimenzionalne realne algebre s dijeljenjem. Spomenimo kako još postoji i neasocijativna realna algebra s dijeljenjem dimenzije 8, tzv. **oktonioni**, koja se obično označava s $\mathbb{O}$. To je algebra koja sadrži jedinicu 1 te sedam linearno nezavisnih elemenata čiji je kvadrat -1. Štoviše, koristeći aparat algebarske topologije, francuski matematičar M. Kervaire i američki matematičar J. Milnor su 1958. godine nezavisno dokazali da su (do na izomorfizam) $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ i $\mathbb{O}$ jedine (ne nužno asocijativne) realne konačnodimenzionalne algebre s dijeljenjem.

Definicija 2.1.11. *Za element x iz F-algebre A kažemo da je **algebarski** ako postoji nenul polinom $f(\omega) \in F[x]$ t.d. je $f(x) = 0$. Ako je svaki element algebre A algebarski, onda za A kažemo da je **algebarska algebra**.*

Napomenimo kako je dosad konačna dimenzionalnost od D korištena samo jednom, i to na početku dokaza leme 2.1.1, kada smo zaključili da je svaki $x \in D$ korijen nenul polinoma u $\mathbb{R}[\omega]$. Sljedeća fundamentalna činjenica slijedi iz dokaza leme 2.1.1:

Lema 2.1.12. *Svaka konačnodimenzionalna algebra je algebarska algebra.*

Dokaz. Skup svih potencija svakog elementa je linearno zavisan. □

Iz dokaza Frobeniusovog teorema zaključujemo da je svaka algebarska realna algebra s dijeljenjem izomorfna $\mathbb{R}$, $\mathbb{C}$ ili $\mathbb{H}$ te je stoga konačnodimenzionalna.

Nakon opisa konačnodimenzionalnih realnih algebri s dijeljenjem, možemo se upitati i što je s kompleksnim? Odgovor možemo potražiti i općenitije, ako umjesto $\mathbb{C}$ promotrimo bilo koje algebarski zatvoreno polje:

Propozicija 2.1.13. *Ako je D konačnodimenzionalna algebra s dijeljenjem nad algebarski zatvorenim poljem F, tada je $D = F$.*

Dokaz. Neka je $x \in D$. Iz leme 2.1.12 vidimo da postoji nenul polinom $f(\omega) \in F[\omega]$ t.d. je $f(x) = 0$. Bez smanjenja općenitosti pretpostavljamo da su vodeći koeficijenti tog polinoma jednaki 1. Kako je F algebarski zatvoreno imamo $f(\omega) = (\omega - \alpha_1) \cdots (\omega - \alpha_r)$ za neke $\alpha_i \in F$. Dakle, slijedi $f(x) = (x-\alpha_1) \cdots (x-\alpha_r) = 0$. Kako je D algebra s dijeljenjem, $x - \alpha_i = 0$ za neki $i \in \mathbb{N}$ pa je stoga $x = \alpha_i \in F$. □

Napomena 2.1.14. *4-dimenzionalna algebra s bazom* $\{1, i, j, k\}$ *te množenjem definiranim u (2.1) i (2.2) ne mora biti samo nad poljem* $\mathbb{R}$*, već nad bilo kojim poljem* F*. No, ako je* $F = \mathbb{C}$*, onda to nije algebra s dijeljenjem. Iz (2.3) vidimo da je algebra s dijeljenjem ako i samo ako za sve* $\alpha_i \in F$*,* $\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 0$ *povlači* $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0$*. Ovaj uvjet je dakako ispunjen u* $\mathbb{R}$*, ali ne u algebarski zatvorenim poljima poput* $\mathbb{C}$*.*

2.2 Prosti prsteni

Definicija 2.2.1. *Prsten R je prost ako je* $R^2 \neq 0$ *te su* 0 *i R jedini ideali od R.*

Uvjet $R^2 \neq 0$, odnosno $xy \neq 0$ za neke $x, y \in R$, je potreban kako bismo isključili patološke slučajeve (jedan takav naveden je u napomeni 2.5).

Primjer 2.2.2. *Svaki prsten s dijeljenjem D je prost. Štoviše, D nema jednostranih ideala različitih od* 0 *i D. Na primjer, neka je I nenul lijevi ideal od A i neka je* $a \in I$*,* $a \neq 0$*. Kako je D prsten s dijeljenjem, a je invertibilan u D pa iz* $Da \subseteq I$ *slijedi* $1 = a^{-1}a \in I$*. Stoga je* $I = D$*.*

Primjer 2.2.3. *Ako je D prsten s dijeljenjem, onda je* $M_n(D)$ *prosti prsten za svaki* $n \in \mathbb{N}$*. Zaista, neka je I nenul ideal od* $M_n(D)$*. Odaberimo* $0 \neq (a_{ij}) \in I$ *te* j, k *takve da* $0 \neq a_{jk} \in M_n(D)$*. Kako je* $(a_{ij}) \in I$ *iz (1.1) vidimo da* $E_{ij}(a_{ij})E_{kl} = a_{jk}E_{il} \in I$ *za sve* $i, l \in \mathbb{N}$*. Kako je D prsten s dijeljenjem,* a_{jk} *je invertibilan u D. Posebno, možemo pisati:* $(da_{jk}^{-1})E_{ii} \cdot a_{jk}E_{il} = dE_{il} \in I$ *za sve* $d \in D$*. S obzirom na to da* dE_{il} *generira* $M_n(D)$ *te* $I \neq 0$ *zaključujemo da je* $I = M_n(D)$*. Dakle, ne postoji netrivijalni ideal od* $M_n(D)$ *pa je stoga* $M_n(D)$ *prosti prsten za svaki* $n \in \mathbb{N}$*.*

Napomena 2.2.4. *U ovom radu fokus je na* ***algebrama****. Umjesto prostih prstena zanimaju nas proste algebre, tj. algebre koje zadovoljavaju uvjete iz definicije 2.2.1. Znamo da ideal neke algebre A mora biti vektorski potprostor, dok u definiciji 2.2.1 govorimo o idealima prstena koji su "samo" aditivne podgrupe. Pretpostavimo da je algebra A takva da su 0 i A jedini ideali algebre A. Pretpostavimo da je I ideal prstena A takav da je* $I \neq A, I \neq 0$*. Tada je AI ideal algebre A pa je* $AI = 0$ *ili* $AI = A$*. Kako je* $AI \subseteq I \neq A$*, jedino možemo zaključiti da* $AI = 0$*, iz čega slijedi da je ideal algebre* $J = \{x \in A \mid Ax = 0\}$ *različit od nule, dakle jednak* $J = A$*. Slijedi,* $A^2 = 0$*. Ova mogućnost isključena je u definiciji 2.2.1. Stoga, algebra A je prosta kao algebra ako i samo ako je A prosta kao prsten.*

Napomena 2.2.5. *Bez pretpostavke $A^2 \neq 0$ moguće je da A ima mnogo ideala prstena, a da nema netrivijalnih ideala algebre. Na primjer, uzmimo 1-dimenzionalnu algebru $A = \mathbb{R}a$ s trivijalnim množenjem, tj. $a^2 = 0$. Onda očito algebra A nema ideala algebre različitih od 0 i A, ali ima ideala prstena (npr. $\mathbb{Z}a$).*

2.3 Centralne algebre

Definicija 2.3.1. *Nenul algebra unitalna algebra A je **centralna** ako se centar od A sastoji samo od skalarnih multipla jedinice, odnosno ako je $Z(A) = \{\lambda 1 : \lambda \in F\}$.*

Lema 2.3.2. *Neka je A unitalna algebra te $n \in \mathbb{N}$. Tada je A centralna ako i samo ako je $M_n(A)$ centralna.*

Dokaz. Ako je $c \in Z(A)$, onda dijagonalna matrica čiji su svi elementi na dijagonali jednaki c leži u $Z(M_n(A))$. Stoga, A je centralna ako je $M_n(A)$ centralan. Pretpostavimo da je A centralna. Odaberimo $C \in Z(M_n(A))$. Kako C komutira sa svakim E_{kl}, $k \neq l$, vidimo da je C dijagonalna matrica sa svim elementima na dijagonali koji su međusobno jednaki. Kako C komutira sa svakim $aE_{11}, a \in A$, zaključujemo da C leži u centru od A te je stoga c skalar. Dakle $M_n(A)$ je centralna. □

Primjer 2.3.3. *Primjenom leme 2.3.2 vidimo da je $M_n(F)$ centralna algebra.*

Primjer 2.3.4. *$\mathbb{H}$ je centralna $\mathbb{R}$ algebra.*

Primjer 2.3.5. *$\mathbb{C}$ je centralna kao $\mathbb{C}$ algebra, ali nije centralna kao $\mathbb{R}$ algebra.*

Iz teorema 2.1.10 slijedi sljedeći korolar:

Korolar 2.3.6. *Konačnodimenzionalna centralna $\mathbb{R}$-algebra s dijeljenjem je izomorfna s $\mathbb{R}$ ili $\mathbb{H}$.*

Glavni fokus idućih poglavlja su *konačnodimenzionalne centralne proste algebre*, koje čine važnu klasu algebra. Kao što vidimo iz prijašnjih primjera, $M_n(F)$ i $\mathbb{H}$ pripadaju toj klasi algebri. Kasnije ćemo vidjeti da je svaka konačnodimenzionalna centralna prosta algebra izomorfna s $M_n(D)$ za neki $n \in \mathbb{N}$ i konačnodimenzionalnu algebru s dijeljenjem D. Kao početak, neke činjenice izvest ćemo direktno iz definicije, bez oslanjanja na samu strukturu tih algebri. U tu svrhu, krenimo s uvođenjem tzv. multiplikacijske algebre.

2.4 Multiplikacijska algebra

Neka je A algebra. Za $a, b \in A$ definiramo preslikavanja $L_a, R_b : A \longrightarrow A$, koja redom nazivamo **lijevo množenje**, odnosno **desno množenje**:

$$L_a(x) := ax, \quad R_b(x) := xb.$$

Ova preslikavanja su očito linearna, dakle pripadaju algebri $\mathrm{End}_F(A)$ svih linearnih operatora iz A u A.

Napomena 2.4.1. *Za sve $a, b \in A; \lambda, \mu \in F$ vrijedi:*

$$L_{ab} = L_a L_b,\ R_{ab} = R_b R_a,$$

$$L_a R_b = R_b L_a,$$

$$L_{\lambda a+\mu b} = \lambda L_a + \mu L_b,\ R_{\lambda a+\mu b} = \lambda R_a + \mu R_b.$$

Odavde slijedi da je

$$M(A) := \{L_{a_1} R_{b_1} + \cdots + L_{a_n} R_{b_n} \mid a_i, b_i \in A, n \in \mathbb{N}\}$$

podalgebra od $\mathrm{End}_F(A)$.

Definicija 2.4.2. *Algebra $M(A)$ naziva se **multiplikacijska algebra od A**.*

Napomena 2.4.3. *Ako je A unitalna algebra, onda L_a=$L_a R_1$ i $R_b = L_1 R_b$ leže u $M(A)$ i u tom slučaju $M(A)$ možemo opisati kao podalgebru od $\mathrm{End}_F(A)$ generiranu svim lijevim i desnim množenjima.*

Napomena 2.4.4. *Neka je $f \in M(A)$. Onda postoje $a_i, b_i \in A$ takvi da $f = \sum_{i=1}^{n} L_{a_i} R_{b_i}$, tj.*

$$f(x) = \sum_{i=1}^{n} a_i x b_i,\ x \in A.$$

Ovi elementi nisu jedinstveni, tj. f možemo prikazati kao sumu operatora oblika $L_a R_b$ na više načina. Ako je $f \neq 0$, onda a_i, b_i možemo odabrati tako da skup svih a_i i skup svih b_i budu linearno nezavisni. Na primjer, ovo je ispunjeno ako zahtijevamo da je n minimalan. Zaista, kada bi, pod ovom pretpostavkom jedan od elemenata bio linearna kombinacija drugih, npr.

$$b_n = \sum_{i=1}^{n-1} \lambda_i b_i,$$

onda bi f bio jednak

$$\sum_{i=1}^{n-1} L_{a_i+\lambda_i a_n} R_{b_i},$$

što je u kontradikciji s minimalnošću od n. Nadalje, ako je $\{u_i \mid i \in I\}$ baza od A, onda svaki R_b možemo izraziti kao linearnu kombinaciju od R_{u_i}, iz čega vidimo da je svaki $f \in M(A)$ konačna suma operatora oblika $L_{a_i} R_{u_i}$ te linearna kombinacija operatora $L_{u_i} R_{u_j}$. Slično, f možemo zapisati kao konačnu sumu operatora oblika $L_{u_i} R_{b_i}$ te štoviše kao linearnu kombinaciju operatora $L_{u_i} R_{u_j}$.

Lema 2.4.5. *Neka je A centralna prosta algebra i neka su $a_i, b_i \in A$ takvi da je*

$$\sum_{i=1}^{n} L_{a_i} R_{b_i} = 0.$$

Ako su a_i linearno nezavisni, onda je svaki $b_i = 0$. Slično, ako su b_i linearno nezavisni, onda je svaki $a_i = 0$.

Dokaz. Razmotrimo slučaj kada su a_i linearno nezavisni; slučaj kada su b_i linearno nezavisni dokazujemo analogno. Pretpostavimo da je $b_n \neq 0$. Kako je A prosta, ideal generiran s b_n je jednak A. Dakle postoje $w_j, z_j \in A$ takvi da je $\sum_{j=1}^{m} w_j b_i z_j = 1$. Stoga je

$$0 = \sum_{j=1}^{m} R_{z_j} \left(\sum_{i=1}^{n} L_{a_i} R_{b_i} \right) R_{w_j} = \sum_{i=1}^{n} L_{a_i} \left(\sum_{j=1}^{m} R_{w_j b_i z_j} \right) = \sum_{i=1}^{n} L_{a_i} R_{c_i},$$

gdje je $c_i = \sum_{j=1}^{m} w_j b_i z_j$, stoga $c_n = 1$. Odavde slijedi da $n > 1$. Možemo pretpostaviti da je n najmanji prirodni broj za kojeg lema ne vrijedi. Kako je

$$0 = \left(\sum_{i=1}^{n} L_{a_i} R_{c_i} \right) R_x - R_x \left(\sum_{i=1}^{n} L_{a_i} R_{c_i} \right) = \sum_{i=1}^{n-1} L_{a_i} R_{xc_i - c_i x},$$

za svaki $x \in A$, slijedi da je $xc_i - c_i x = 0$ za sve $x \in A$, odnosno $c_i \in Z(A) = F$. Odavde slijedi,

$$0 = \sum_{i=1}^{n} L_{a_i} R_{c_i} = L_{c_1 a_1 + \cdots + c_n a_n}.$$

Posebno

$$0 = L_{c_1 a_1 + \cdots + c_n a_n}(1) = c_1 a_1 + \cdots + c_n a_n.$$

Kako je $c_n = 1 \neq 0$, dolazimo u kontradikciju s pretpostavkom da su a_i linearno nezavisni. □

Napomena 2.4.6. *Prisjetimo se da iz* $[A : F] = d$ *slijedi* $[\mathrm{End}_F(A) : F] = d^2$.

Lema 2.4.7. *Ako je A konačnodimenzionalna centralna prosta algebra, onda* $M(A) = \mathrm{End}_F(A)$.

Dokaz. Neka je $\{u_1, \ldots, u_d\}$ baza od A. Iz leme 2.4.5 slijedi da su operatori $L_{u_i}R_{u_j}, 1 \leq i, j \leq d$ linearno nezavisni. Ovo je jasno ako zapišemo $\sum_{i,j=1}^{d} \lambda_{ij} L_{u_i} R_{u_j}$ kao $\sum_{i=1}^{d} L_{u_i} R_{b_i}$, gdje je $b_i = \sum_{j=1}^{d} \lambda_{ij} u_j$. Stoga je

$$[M(A) : F] \geq d^2 = [\mathrm{End}_F(A) : F],$$

pa iz prethodne napomene slijedi $M(A) = \mathrm{End}_F(A)$. □

2.5 Automorfizmi centralnih prostih algebri

U unitalnim prstenima (i algebrama) postoji kanonski način konstrukcije automorfizama; svaki invertibilni element može generirati unutarnji automorfizam:

Definicija 2.5.1. *Automorfizam* ϕ *unitalnog prstena R nazivamo* ***unutarnji automorfizam*** *ako postoji invertibilni element* $a \in R$ *takav da* $\phi(x) = axa^{-1}$ *za sve* $x \in R$.

Automorfizam koji nije unutarnji nazivamo ***vanjski automorfizam***.

Navedimo nekoliko primjera takvih automorfizama.

Primjer 2.5.2. *Konjugacija* $z \mapsto \bar{z}$ *je automorfizam* $\mathbb{R}$*-algebre* $\mathbb{C}$. *Jasno, konjugacija je vanjski automorfizam jer je identiteta očito jedini unutarnji automorfizam komutativnog prstena. Spomenimo još da je element od* $\mathrm{End}_{\mathbb{R}}(\mathbb{C})$, *ali nije u* $M(\mathbb{C})$. *Stoga, u lemi 2.4.7 ne možemo izostaviti pretpostavku da je A centralna.*

Primjer 2.5.3. *Za svaki* $\alpha \in F \setminus \{0\}$, $f(\omega) \mapsto f(\omega + \alpha)$ *je vanjski automorfizam algebre* $F[\omega]$.

Primjer 2.5.4. *Neka je S prsten i neka je* $R = S \times S$ *direktni produkt dviju kopija od S. Tada je* $(s, t) \mapsto (t, s)$ *vanjski automorfizam od R.*

Teorem 2.5.5. *(Skolem-Noether) Svaki automorfizam konačnodimenzionalne centralne proste algebre A je unutarnji.*

Dokaz. Neka je ϕ automorfizam od A. Iz leme 2.4.7 vidimo da je

$$\phi = \sum_{i=1}^{n} L_{a_i} R_{b_i}$$

za neke $a_i, b_i \in A$. Možemo pretpostaviti da je $a_1 \neq 0$ i da su b_i linearno nezavisni (napomena 2.4.4). Kako je ϕ multiplikativan, imamo

$$L_{\phi(x)}\phi = \phi L_x \quad \text{za svaki } x \in A.$$

Odavde slijedi

$$\sum_{i=1}^{n} L_{\phi(x)a_i - a_i x} R_{b_i} = 0.$$

Iz leme 2.4.5 slijedi da

$$\phi(x)a_1 - a_1 x = 0, \quad x \in A. \tag{2.5}$$

Pokažimo još da je a_1 invertibilan. Kako je A prosta, postoje $w_j, z_j \in A$ takvi da

$$\sum_{j=1}^{m} w_j a_1 z_j = 1. \tag{2.6}$$

Kako iz (2.5) slijedi $xa_1 = a_1\phi^{-1}(x)$ za svaki $x \in A$, sumu u (2.6) možemo zapisati kao:

$$\left(\sum_{j=1}^{m} w_j \phi(z_j)\right) a_1 = 1 \qquad \text{i} \qquad a_1 \left(\sum_{j=1}^{m} \phi^{-1}(w_j) z_j\right) = 1.$$

Dakle, a_1 ima lijevi i desni inverz, odakle slijedi da je a_1 invertibilan. □

Napomena 2.5.6. *Za konačnodimenzionalne unitalne algebre vrijede sljedeće tvrdnje:*

(a) Desni inverz elementa je automatski ujedno i lijevi inverz elementa, odnosno $ab = 1$ povlači $ba = 1$. Ovo možemo dokazati tako da primijenimo lemu 2.1.12 kako bismo dobili postoji nenul polinom $f(\omega) \in F[\omega]$, takav da je $f(a) = 0$. Pretpostavimo da f ima najmanji stupanj među svim takvim polinomima. Tada možemo pisati $f(a) = 0$ kao $ag(a) = \alpha$, gdje je α negativni konstantni član od f, a $g(\omega) \in F[\omega]$ je nenul polinom stupnja manjeg od $f(\omega)$, takav da $g(a) \neq 0$. Ako je $\alpha \neq 0$, onda je a invertibilan, $a^{-1} = \alpha^{-1}g(a)$. Ako je $\alpha = 0$, onda $ag(a) = g(a)a = 0$ i a nema lijevih ni desnih inverza.

(b) Iz diskusije u (a) posebno vidimo da je svaki nenul element $a \in A$ ili invertibilan ili djelitelj nule.

(c) Nenul podalgebra A neke konačnodimenzionalne algebre s dijeljenjem D je također algebra s dijeljenjem. Zaista, uzmimo $0 \neq a \in A$. Onda je $1 \in A$ jer je a algebarski i invertibilan. Nadalje, iz (a) vidimo da $a^{-1} = \alpha^{-1}g(a) \in A$.

2.6 Maksimalna potpolja

Ako je K podalgebra unitalne F-algebre A polje i vrijedi $K \supseteq F$ (tj. K sadrži jedinicu od A), onda K nazivamo **potpolje** od A. U tom slučaju A možemo promatrati kao vektorski prostor nad K.

Napomena 2.6.1. *Ako je K potpolje konačnodimenzionalne unitalne algebre A, onda vrijedi:*

$$[A : F] = [A : K][K : F].$$

Ova formula je specijalni slučaj gdje je A proširenje polja K. Zaista, ako je $\{k_i \mid i = 1, \ldots, m\}$ baza od K nad F i $\{a_j \mid j = 1, \ldots, n\}$ je baza od A nad K, onda lako vidimo da je $\{k_i a_j \mid i = 1, \ldots, m, j = 1, \ldots, n\}$ baza od A nad F.

Definicija 2.6.2. *Potpolje koje nije strogo sadržano ni u jednom većem potpolju od A nazivamo **maksimalno potpolje** od A.*

Primjer 2.6.3. *Potpolja $\mathbb{R} \oplus \mathbb{R}i$, $\mathbb{R} \oplus \mathbb{R}j$ i $\mathbb{R} \oplus \mathbb{R}k$ su maksimalna potpolja od $\mathbb{H}$. Sva ta polja su 2-dimenzionalna te izomorfna s $\mathbb{C}$.*

Napomena 2.6.4. *Ako je K potpolje od A, onda je $R_u \in \mathrm{End}_K(A)$ za svaki $u \in A$. Zaista, $R_u(kx) = kxu = kR_u(x)$ za sve $k \in K$, $x \in A$. Nadalje, za $f \in \mathrm{End}_K(A)$, skalarni multipli kf, $k \in K$, od mogu biti interpretirani kao operator $L_k f$.*

Teorem 2.6.5. *Neka je D konačnodimenzionalna centralna algebra s dijeljenjem nad poljem F. Ako je K maksimalno potpolje od D, onda je $[D : F] = [K : F]^2$.*

Dokaz. Neka je $\{u_1, \ldots, u_d\}$ baza F-algebre D. Tvrdimo da je $\{R_{u_1}, \ldots, R_{u_d}\}$ baza K-algebre $\mathrm{End}_K(D)$. Iz leme 2.4.5 slijedi da je ovaj skup linearno nezavisan pa je dovoljno pokazati da razapinje $\mathrm{End}_K(D)$. Neka je $f \in \mathrm{End}_K(D)$. Posebno, $f \in \mathrm{End}_F(D)$ pa iz leme 2.4.7 (i napomene 2.4.4) slijedi da

$$f = \sum_{i=1}^{d} L_{a_i} R_{u_i}$$

za neke $a_i \in D$. Kako je f K-linearan, $fL_k = L_k f$ vrijedi za svaki $k \in K$ pa imamo:

$$\sum_{i=1}^{d} L_{a_i k - k a_i} R_{u_i} = 0.$$

Iz leme 2.4.5 vidimo da $a_i k - k a_i = 0$ za svaki i i svaki $k \in K$, iz čega slijedi da $a_i \in K$, jer bi inače podalgebra generirana od a_i i K bilo polje veće od K (napomena 2.5.6 (c)). Stoga, f je K-linearna kombinacija R_{u_i}.

Prema tome,

$$[D : F] = d = [\mathrm{End}_K(D) : K] = [D : K]^2.$$

S druge strane, iz napomene 2.6.1 slijedi

$$[D : F] = [D : K][K : F],$$

pa je stoga $[D : F] = [K : F]^2$. □

Korolar 2.6.6. *Dimenzija konačnodimenzionalne centralne algebre s dijeljenjem je potpuni kvadrat.*

Dokaz. Konačnodimenzionalna centralna prosta algebra sadrži maksimalna potpolja. Doista, to su točno potpolja maksimalnih dimenzija pa zaključak slijedi iz teorema 2.6.5. □

Poglavlje 3

Struktura konačnodimenzionalnih algebri

Ovo poglavlje, kao i prošlo, u konačnici sadrži dokaz drugog velikog teorema (odnosno u ovom slučaju dva) koji nam opisuju strukturu tzv. poluprim konačnodimenzionalnih algebri. Riječ je o Wedderburnovim strukturalnim teoremima. Koncept rada nastavljamo na isti način, dakle s direktnom izgradnjom teorije koja nam je potrebna za dokaz željenog teorema umjesto izgradnje neke općenite matematičke teorije iz koje bismo izveli same teoreme.

Napomena 3.0.1. *Prisjetimo se, ako je R prsten, tada za ideale $I, J \trianglelefteq R$ definirajmo njihov zbroj $I + J$ kao najmanji ideal u R koji sadrži $I \cup J$ te njihov produkt IJ kao najmanji ideal koji sadrži sve produkte elemenata xy, gdje su $x \in I, y \in J$; tj.,*

$$I + J := \langle I \cup J \rangle,$$

$$IJ := \langle xy \mid x \in I, y \in J \rangle.$$

Analogno, ako su $I_1, \ldots, I_n \trianglelefteq R$ ideali, definiramo

$$I_1 + \ldots + I_n := \langle I_1 \cup \ldots \cup I_n \rangle,$$

$$I_1 \cdots I_n := \langle x_1 \cdots x_n \mid x_j \in I_j \rangle.$$

3.1 Nilpotentni ideali

Definicija 3.1.1. *Ideal I prstena R je **nilpotentni ideal** ako postoji $n \in \mathbb{N}$ takav da $I^n = 0$.*

Uvjet $I^n = 0$ znači da je $u_1u_2\cdots u_n = 0$ za sve $u_i \in I$.

Definicija 3.1.2. *Element a prstena R nazivamo **nilpotentni element** ako postoji $n \in \mathbb{N}$ takav da je $a^n = 0$.*

Definicija 3.1.3. *Ideal I prstena R nazivamo **nil ideal** ako su svi elementi u I nilpotentni.*

Očito, nilpotentni ideal je nil ideal. Može se pokazati da obrat općenito ne vrijedi.

Primjer 3.1.4. *Uzmimo bilo koju aditivnu grupu R uz trivijalni produkt $xy = 0$ za sve $x, y \in R$. Onda je $R^2 = 0$.*

Primjer 3.1.5. *Nilpotentni element koji leži u centru $Z(R)$ prstena R očito generira nilpotentni ideal. Jednostavan primjer takvog elementa možemo dobiti tako da uzmemo direktni produkt prstena iz primjera 3.1.4 s bilo kojim drugim prstenom.*

Primjer 3.1.6. *Neka je $A = T_n(F)$ algebra svih gornje trokutastih $n\times n$ matrica nad poljem F, tj. matrica kojima su elementi ispod glavne dijagonale nula. Neka je N skup svih strogo gornje trokutastih matrica, tj. gornje trokutastih matrica kojima su i elementi na glavnoj dijagonali nula. Tada je N ideal od A takav da $N^n = 0$ i $N^{n-1} \neq 0$. Možemo pronaći razne ideale od A koji su sadržani u N te su stoga nilpotentni. Na primjer, skup svih matrica I, koje na mjestu $(1, n)$ imaju proizvoljan element, a na svim ostalim mjestima nulu je ideal od A koji zadovoljava $I^2 = 0$.*

Napomena 3.1.7. ***Nilpotentni jednostrani ideali** definirani su na isti način kao i nilpotentni ideali. Ako je L nilpontetni lijevi ideal od R, onda je L sadržan u dvostranom nilpotentnom idealu $L + LR$. Naime, lako se vidi da $L^n = 0$ implicira $(L + LR)^n = 0$. Slično, svaki desni nilpotentni ideal je sadržan u nilpotentnom idealu.*

Lema 3.1.8. *Suma dva nilpotentna ideala je nilpotentan ideal.*

Dokaz. Neka su I, J ideali takvi da $I^n = 0$ i $J^m = 0$. Tvrdimo da $(I+J)^{n+m-1} = 0$. Odnosno, produkt $n+m-1$ elemenata oblika $u+v$, $u \in I$, $v \in J$ je 0. Takav produkt možemo napisati kao sumu produkata $w = w_1w_2\cdots w_{n+m-1}$, gdje svaki $w_i \in I \cup J$. Ako je barem n članova sume u I, onda $w = 0$ jer je $I^n = 0$. Ako je broj w_i-ova koji pripadaju I manji od n, onda ih barem m leži u J pa stoga $w = 0$ jer $J^m = 0$. □

Definicija 3.1.9. *Ideal koji nije potpuno sadržan u većem nilpotentnom idealu nazivamo **maksimalni nilpotentni ideal**.*

Lema 3.1.10. *Ako prsten R ima maksimalan nilpotentni ideal N, onda N sadrži sve nilpotentne ideale od R.*

Dokaz. Pretpostavimo da je I neki nilpotentni ideal od R. Iz leme 3.1.8 vidimo da je $I + N$ također nilpotentni ideal. Kako je N maksimalni nilpotentni ideal od R i $N \subseteq I + N$ mora vrijediti $I + N = N$. Stoga je $I \subseteq N$. □

Napomena 3.1.11. *Dakle, ako u prstenu R postoji maksimalni nilpotentni ideal, onda je on jedinstven i jednak sumi svih nilpotentnih ideala. To se posebno odnosi na slučaj kada je $R = A$ konačnodimenzionalna algebra. Naime, u tom slučaju A sadrži bar jedan nilpotentni ideal (sigurno sadrži nulideal). Stoga je skup svih nilpotentnih ideala u A neprazan te sadrži element maksimalne dimenzije, što je očito maksimalni nilpotentni ideal.*

Definicija 3.1.12. *Maksimalni nilpotentni ideal konačnodimenzionalne algebre A nazivamo* ***radikal*** *od A. Ako je radikal od A jednak* 0*, tada za A kažemo da je* ***poluprosta algebra****.*

Primjer 3.1.13. *Radikal algebre $A = T_n(F)$ iz primjera 3.1.6 je N, skup svih strogo gornje trokutastih matrica. Zaista, N je nilpotentni ideal od A i bilo koji ideal od A koji strogo sadrži N ne može biti nilpotenti ideal jer mora sadržavati nenul dijagonalnu matricu.*

3.2 Prim i poluprim prsteni

Definicija 3.2.1. *Prsten R nazivamo* ***domena*** *ako za sve $a, b \in R$, $ab = 0$ povlači $a = 0$ ili $b = 0$.*

Drugim riječima, R je domena ako nema lijevih (ili desnih) djelitelja nule. Ekvivalentno, R je domena ako ima *pravilo skraćivanja*:
Ako je $a \neq 0$, onda $ab = ac$ i $ba = ca$ povlači $b = c$.

Lema 3.2.2. *Neka je R prsten. Sljedeće tvrdnje su međusobno ekvivalentne:*

(i) Za svaki $a, b \in R$, $aRb = 0$ povlači $a = 0$ ili $b = 0$.

(ii) Za sve lijeve ideale I i J od R, $IJ = 0$ povlači $I = 0$ ili $J = 0$.

(iii) Za sve desne ideale I i J od R, $IJ = 0$ povlači $I = 0$ ili $J = 0$.

(iv) Za sve ideale I i J od R, $IJ = 0$ povlači $I = 0$ ili $J = 0$.

Dokaz.
(i) $\Rightarrow$ (ii) Pretpostavimo da za sve $a, b \in R$ iz $aRb = 0$ slijedi $a = 0$ ili $b = 0$. Neka su I i J lijevi ideali u R takvi da je $IJ = 0$. Tada je $RJ \subseteq J$ pa je $IRJ = 0$. Prema pretpostavci, slijedi da je $I = 0$ ili $J = 0$.

(i) $\Rightarrow$ (iii) pokazuje se analogno.
(ii) $\Rightarrow$ (iv), (iii) $\Rightarrow$ (iv) je trivijalno zadovoljeno.

(iv) $\Rightarrow$ (i) Pretpostavimo da za svaka dva ideala $I, J \trianglelefteq R$ iz $IJ = 0$ slijedi $I = 0$ ili $J = 0$. Neka su $a, b \in R$ takvi da je $aRb = 0$. Posebno, produkt ideala je RaR i RbR je 0 pa je jedan od njih 0. Ako je npr. $RaR = 0$, slijedi da su Ra i aR obostrani ideali takvi da $Ra \cdot R = R \cdot aR = 0$. Prema (iv) vidimo da $Ra = aR = 0$. Sada, posebno, $\mathbb{Z}a$ je ideal od R koji zadovoljava $\mathbb{Z}a \cdot R = 0$ te iz (iv) slijedi da $a = 0$. Stoga (iv) povlači (i). □

Definicija 3.2.3. *Prsten R je **prim** prsten ako zadovoljava jedan (stoga i sve) uvjete leme 3.2.2.*

Lema 3.2.4. *Komutativni prsten je prim ako i samo ako je domena.*

Dokaz. Dovoljno je primijetiti da $ab = 0$ povlači $aRb = 0$ ako je R komutativan. □

Lema 3.2.5. *Neka je R prsten. Sljedeće tvrdnje su ekvivalentne:*

(i) Za sve $a \in R$, $aRa = 0$ povlači $a = 0$.

(ii) Za sve lijeve ideale I id R, $I^2 = 0$ povlači $I = 0$.

(iii) Za sve desne ideale I od R, $I^2 = 0$ povlači $I = 0$.

(iv) Za sve ideale I od R, $I^2 = 0$ povlači $I = 0$.

(v) R nema nenul nilpotetnih ideala.

Dokaz.
(i) $\Rightarrow$ (ii): Pretpostavimo da za sve $a \in R$, aRa povlači $a = 0$ te neka je I lijevi ideal u R takav da je $I^2 = 0$. Tada za svaki $a \in I$ vrijedi $aRa \subseteq aI \subseteq I^2 = 0$ pa je prema (i) $a = 0$. Dakle, $I = 0$. (i) $\Rightarrow$ (iii) pokazuje se analogno.
(ii) $\Rightarrow$ (iv), (iii) $\Rightarrow$ (iv) je trivijalno zadovoljeno.
Pokažimo još (iv) $\Leftrightarrow$ (v).
(v) $\Rightarrow$ (iv) je trivijalno zadovoljen.
(iv) $\Rightarrow$ (v) Pretpostavimo da je I ideal od R takav da vrijedi $I^n = 0, n > 1$. Tada je $(I^{n-1})^2 = 0$ pa iz pretpostavke slijedi $I^{n-1} = 0$. Koristeći induktivni argument dobivamo $I = 0$. □

Definicija 3.2.6. *Prsten R nazivamo **poluprim** prstenom ako zadovoljava jedan (stoga i sve) tvrdnje iz leme 3.2.5.*

Primijetimo jedan očiti analogon lemi 3.2.4.

Lema 3.2.7. *Komutativni prsten je poluprim ako i samo ako nema nenul nilpotentnih elemenata.*

Napomena 3.2.8. *Ako je A algebra te su I, J ideali prstena od A takvi da $IJ = 0$, onda su linearne ljuske od I i J ideali algebre čiji je produkt 0. Stoga, slijedi da* ***prim algebru*** *možemo definirati i kao algebru koja je prim kao prsten ili algebru u kojoj je produkt bilo koja dva nenul ideala algebre različit od nule. Slična napomena vrijedi i za* ***poluprim algebre*** *(usporediti s napomenom 2.5).*

Napomena 3.2.9. *Neka je I nenul ideal prim prstena R. Ako su $a, b \in R$ takvi da $aIb = 0$, onda $aRuRb = 0$ za svaki $u \in I$. Koristeći (i) iz leme 3.2.2 dvaput, slijedi da $a = 0$ ili $b = 0$. Posebno, ideal prim prstena ponovo je prim prsten. Slično, ideal poluprim prstena je poluprim prsten.*

Korolar 3.2.10. *Konačnodimenzionalna algebra A je poluprim ako i samo ako je poluprosta.*

Dokaz. Neka je N radikal od A. Ako je A poluprim, onda prema lemi 3.2.5 A nema nilpotentnih ideala. Stoga je $N = 0$, odnosno A je poluprosta. Obratno, pretpostavimo da je $N = 0$ i neka je I nilpotentni ideal od A. Kako je N najveći nilpotentni ideal od A, slijedi $I \subseteq N$. Dakle $I = 0$ pa je A poluprim prema lemi 3.2.5. □

Sljedeće relacije između dosad uvedenih klasa prstena slijede iz definicija:

$$\begin{aligned} \text{prsten s dijeljenjem} &\implies \text{prost i domena,} \\ \text{prost} &\implies \text{prim,} \\ \text{domena} &\implies \text{prim,} \\ \text{prim} &\implies \text{poluprim.} \end{aligned}$$

Primjer 3.2.11. *Prsten $\mathbb{Z}$ je domena koja nije prosti prsten.*

Primjer 3.2.12. *Matrični prsten $M_n(F)$, $n \geq 2$, je prost, ali nije domena.*

Primjer 3.2.13. *Matrični prsten $M_n(\mathbb{Z})$, $n \geq 2$, je prim, ali nije niti domena niti prost prsten. Očiti (i štoviše jedini) primjeri njegovih ideala su $M_n(k\mathbb{Z})$ za $k \geq 0$.*

3.3 Unitizacija

Neka je A F-algebra. Skup $F \times A$ postaje F-algebra, koju označavamo s $A^\sharp$, uz operacije

$$(\lambda, x) + (\mu, y) := (\lambda + \mu, x + y),$$

$$\mu(\lambda, x) := (\mu\lambda, \mu x),$$
$$(\lambda, x)(\mu, y) := (\lambda\mu, \mu x + \lambda y + xy),$$

gdje su $\lambda, \mu \in F$ te $x, y \in A$. Tada A postaje podalgebra od $A^\sharp$ nakon što ju identificiramo sa slikom monomorfizma $x \mapsto (0, x)$. Štoviše, A zapravo ideal od $A^\sharp$. Također primijetimo da je $A^\sharp$ unitalna algebra s jedinicom $(1, 0)$.

Definicija 3.3.1. *Algebra $A^\sharp$ naziva se **unitizacija** od A.*

Lema 3.3.2. *Ako je A neunitalna prim algebra, onda je $A^\sharp$ također prim algebra.*

Dokaz. Neka su $(\lambda, a), (\mu, b) \in A^\sharp$ takvi da zadovoljavaju $(\lambda, a)A^\sharp(\mu, b) = 0$. Onda je posebno $(\lambda, a)(1, 0)(\mu, b) = 0$ pa stoga $\lambda = 0$ ili $\mu = 0$. Promotrimo slučaj kada $\lambda = 0$; slučaj kada je $\mu = 0$ je analogan. Možemo pretpostaviti da je $a \neq 0$. Iz $(0, a)(0, x)(\mu, b) = 0$ zaključujemo da $\mu ax + axb = 0$ za sve $x \in A$. Pretpostavimo također da je $\mu \neq 0$, jer je inače $aAb = 0$ pa onda i $b = 0$. Definirajmo $e := -\mu^{-1}b$. Tada imamo $ax = axe$ za svaki $x \in A$. Prema tome, $a(xy)e = axy = (axe)y$ za sve $x, y \in A$. Ovo možemo zapisati kao

$$ax(y - ye) = 0 = ax(y - ey).$$

Kako je A prim algebra, slijedi da $y = ye$ i $y = ey$ za sve $y \in A$, što je u kontradikciji s pretpostavkom da je A algebra bez jedinice. □

3.4 Matrične jedinice

Standardne matrične jedinice E_{ij} definirali smo ranije u definiciji 1.0.4. Uvedimo i njihovu apstraktnu generalizaciju:

Definicija 3.4.1. *Neka je R unitalni prsten i neka je $n \in \mathbb{N}$. Skup $\{e_{ij} \in R \mid 1 \leq i, j \leq n\}$ nazivamo $n \times n$ **sustav matričnih jedinica** ako je*

$$e_{11} + e_{22} + \cdots + e_{nn} = 1$$

i

$$e_{ij}e_{kl} = \delta_{jk}e_{il}$$

za sve $1 \leq i, j, k, l \leq n$, gdje je δ_{jk} "Kroneckerov simbol", tj.

$$\delta_{jk} = \begin{cases} 1 \text{ ako je } j = k \\ 0 \text{ ako je } j \neq k \end{cases}.$$

Matrične jedinice e_{ij} s $i \neq j$ bitno se razlikuju od matričnih jedinica e_{ii}. Matrične jedinice oblika $e_{ij}, i \neq j$ su nilpotetni elementi jer zadovoljavaju jednakost $e_{ij}^2 = 0$, dok za elemente oblika $e_{ii}, i \in \mathbb{N}$ vrijedi $e_{ii}^2 = e_{ii}$.

Definicija 3.4.2. *Element e prstena R je **idempotentan** ako je $e^2 = e$. Idempotenti e i f su **ortogonalni** ako vrijedi $ef = fe = 0$.*

Lema 3.4.3. *Neka je A unitalna algebra. Ako A sadrži $n \times n$ sustav matričnih jedinica $\{e_{ij} \in A \mid 1 \leq i, j \leq n\}$, onda je $A \cong M_n(S_t)$, gdje je $S_t := e_{tt}Ae_{tt}$ za $t = 1, \ldots, n$.*

Dokaz. Neka je $\phi : A \to M_n(S_t)$ funkcija definirana s:

$$\phi(a) := (a_{ij}),$$

gdje je

$$a_{ij} := e_{ti}ae_{jt} = e_{tt}e_{ti}ae_{jt}e_{tt} \in S_t.$$

Dokažimo da je ϕ izomorfizam algebri.

Linearnost: Trebamo dokazati da vrijedi $\phi(\lambda a + \mu b) = \lambda\phi(a) + \mu\phi(b)$, za sve $a, b \in A$ te $\lambda, \mu \in F$. Zaista, (i, j)-ta vrijednost od $\phi(\lambda a + \mu b)$ je

$$e_{ti}(\lambda a + \mu b)e_{jt} = \lambda e_{ti}ae_{jt} + \mu e_{ti}be_{jt},$$

što je točno (i, j)-ta vrijednost od $\lambda\phi(a) + \mu\phi(b)$.

Multiplikativnost: Trebamo dokazati da vrijedi $\phi(ab) = \phi(a)\phi(b)$, za sve $a, b \in A$. Zaista, (i, j)-ta vrijednost od $\phi(ab)$ jednaka je

$$\begin{aligned} e_{ti}abe_{jt} &= e_{ti}a1be_{jt} = e_{ti}a\left(\sum_{k=1}^{n} e_{kk}\right)be_{jt} = e_{ti}a\left(\sum_{k=1}^{n} e_{kt}e_{tk}\right)be_{jt} \\ &= \sum_{k=1}^{n} e_{ti}ae_{kt}e_{tk}be_{jt}, \end{aligned}$$

što je točno (i, j)-ta vrijednost od $\phi(a)\phi(b)$.

Injektivnost: Dovoljno je dokazati da je jezgra od ϕ trivijalna. Pretpostavimo stoga da je $\phi(a) = 0$. Tada je

$$e_{ii}ae_{jj} = e_{it}a_{ij}e_{tj} = 0$$

za sve $i, j = 1, \ldots n$. Kako je $\sum_{i=1}^{n} e_{ii} = 1$, slijedi $a = 0$. Dakle, $\ker\phi = 0$.

Surjektivnost: Za proizvoljan $a \in A$ te $k, l = 1 \ldots, n$, vidimo da je $\phi(e_{k1}ae_{1l})$ matrica iz $M_n(S_t)$ koja na (k, l)-tom mjestu ima element $e_{tt}ae_{tt}$, a na svim ostalim mjestima nulu. Kako se svaki element od S_t može napisati kao konačna suma elemenata tog oblika, te kako je $\phi(A)$ podalgebra (posebno potprostor) od $M_n(S_t)$, zaključujemo da je $\phi(A) = M_n(S_t)$, odnosno ϕ je surjektivna funkcija.

Dakle, $A \cong M_n(S_t)$. □

3.5 Idempotenti

Neka je e idempotent u prstenu R.

Kao što smo vidjeli u prijašnjem dijelu rada, eRe nam je vrlo zanimljiv potprsten od R. eRe nazivamo **kutni prsten** koji odgovara e. Kutni prsten eRe ima jedinicu, čak i ako R nema; jedinica mu je jednaka e. Radi jednostavnosti, u daljnjem će R označavati unitalni prsten, a e **netrivijalni idempotent**, odnosno idempotent različit od 0_R i 1_R. Tada da je i

$$f := 1 - e$$

također netrivijalni idempotent u R. Nadalje, e i f su ortogonalni i njihova suma je 1. Primjer takvog para idempotenta su matrične jedinice e_{11} i e_{22} u 2×2 matričnom prstenu $M_2(R)$.

Pretpostavimo da je $ex_1e + ex_2f + fx_3e + fx_4f = 0$ za neke $x_i \in R$. Množenjem s lijeva i s desna s e dobivamo $ex_1e = 0$. Ostali članovi su nula jer su e i f ortogonalni. S druge strane, kako svaki $x \in R$ možemo zapisati kao

$$x = exe + exf + fxe + fxf,$$

slijedi da je

$$R = eRe \oplus eRf \oplus fRe \oplus fRf, \tag{3.1}$$

kao direktna suma Abelovih grupa.

Dekompoziciju (3.1) nazivamo **Peirceova dekompozicija** od R (s obzirom na e). Definirajmo

$$R_{11} := eRe,\ R_{12} := eRf,\ R_{21} := fRe,\ R_{22} := fRf.$$

Tada su R_{11} i R_{22} kutni prsteni koji odgovaraju e i f, a produkt svaka dva elementa u R_{12}, odnosno R_{21} je nula. Nadalje, vrijedi

$$R_{ij}R_{kl} \subseteq \delta_{jk}R_{il}$$

za sve $1 \leq i, j, k, l \leq 2$.

Primijetimo da ako u prstenu imamo netrivijalni idempotent e, možemo pomoću elementa $f = 1 - e$ dobiti strukturu koja izgleda kao 2×2 matrice. Općenito, prsten R s netrivijalnim idempotentom e nije izomorfan 2×2 matričnom prstenu. Za takvu tvrdnju potrebne su nam dodatne pretpostavke, tj. da su jednadžbe

$$exfye = e \text{ i } fyexf = f$$

rješive u R. Naime, u tom slučaju možemo definiramti elemente

$$e_{11} := e,\ e_{12} := exf,\ e_{21} := fye,\ e_{22} := f,$$

koji čine 2×2 sustav matričnih jedinica od R. Prema lemi 3.4.3 vrijedi $R \cong M_2(eRe)$.

Postoji mnogo primjera prstena bez netrivijalnih idempotenta, na primjer domene ili prsteni s dijeljenjem. Postojanje jednog netrivijalnog idempotenta povlači postojanje "mnogo" takvih elemenata, barem u slučaju kada su sumandi eRf i fRe iz Peirceove dekompozicije različiti od nule. Ako je e idempotent, onda su $e + exf$ i $e + fxe$ također idempotenti za svaki $x \in R$. Također $p^{-1}ep$ je idempotent za svaki invertibilni element $p \in R$.

Ovakva razmatranja nemaju smisla ako je e **centralni idempotent**, odnosno idempotent iz centra $Z(R)$ od R. U tom slučaju $eRf = fRe = 0$ pa se Peirceova dekompozicija reducira na dva sumanda: $I := eR = eRe$ i $J := fR = fRf$. Jasno, I i J su ideali od R, $R = I \oplus J$ te $R \cong I \times J$ uz izomorfizam $x \mapsto (ex, fx)$.

Ranije smo pretpostavili da je R unitalni prsten, što nam je omogućilo definiranje idempotenta $f = 1 - e$. Možemo vidjeti da nam jedinica nije nužna u prethodno opisanoj konstrukciji. Naime, primijetimo da nismo radili direktno s elementom f nego s produktom elemenata iz R s f. Ako pretpostavimo da R nema jedinicu, onda pišemo $x - ex$ umjesto fx, odnosno $x - ex - xe + exe$ umjesto fxf. Tada većina činjenica iz ranije diskusije itekako ima smisla. Konkretno, Peirceova dekompozicija je i dalje moguća, ali zbog nedostatka jedinice formule koje moramo koristiti su kompliciranije. Međutim, tvrdnje koje se tiču centralnih idempotenata trebaju samo male promjene: Ako je e centralni idempotent u R, onda su $I = eR$ i $J = \{x - ex \mid x \in R\}$ ideali od R takvi da vrijedi

$$R = I \oplus J \cong I \times J.$$

Promatramo li I kao prsten, vidimo da je e njegova jedinica. Sami ideali su rijetko unitalni prsteni. Zapravo, samo oni generirani centralnim idempotentima su upravo takvi prsteni.

Lema 3.5.1. *Neka je I ideal prstena R. Ako je I unitalni prsten, onda je njegova jedinica e centralni idempotent u R i $I = eR$. Nadalje, postoji ideal J od R takav da je $R = I \oplus J$. Štoviše, $R \cong I \times J$.*

Dokaz. Kako je $e \in I$, imamo $eR \subseteq I$ te obratno $I = eI \subseteq eR$. Stoga $I = eR$. Nadalje, kako je $ex, xe \in I$ za svaki $x \in R$, imamo $ex = (ex)e$ i $xe = e(xe)$. Slijedi da $ex = xe$ pa je e centralni idempotent. Zaključak slijedi iz prethodne diskusije, prije iskaza leme. □

Ako pretpostavimo da je R unitalni prsten, onda možemo iskazati obrat leme 3.5.1: Ako su I i J ideali od R takvi da $R = I \oplus J$, onda postoji centralni idempotent $e \in R$ takav da $I = eR$ i $J = (1 - e)R$ (I i J su unitalni prsteni). Za dokaz samo možemo uzeti elemente $e \in I$ i $f \in J$ takve da je $e + f = 1$ te provjeriti da e (odnosno f) ima željena svojstva.

3.6 Minimalni lijevi ideali

U slučajevima kada razmatramo jednostrane ideale, u ovom radu razmatrat ćemo lijeve ideale. Situacija je analogna i za desne ideale.

Definicija 3.6.1. *Lijevi ideal L prstena R nazivamo **minimalni lijevi ideal** ako je $L \neq 0$ te ako niti jedan nenul lijevi ideal nije pravi podskup od R.*

Minimalni desni ideali te **minimalni dvostrani ideali** definirani su na analogan način.

Minimalni ideali za algebre definirani su na analogan način kao i minimalni ideali prstena.

Primjer 3.6.2. *Jedini minimalni lijevi ideal prstena s dijeljenjem D je sam D.*

Primjer 3.6.3. *Neka je $R = M_n(D)$ prsten s dijeljenjem i neka je L skup matrica u R koje imaju proizvoljan element u i-tom stupcu i nule u svim ostalim stupcima. Lako se vidi da je L minimalni lijevi ideal od R. Također, napomenimo da je $L = RE_{ii}$ gdje je E_{ii} standardna matrična jedinica i da je $E_{ii}RE_{ii} = \{dE_{ii} \mid d \in D\}$ potprsten s dijeljenjem od R izomorfan s D.*

Lema 3.6.4. *Ako je L minimalni lijevi ideal poluprim prstena R, onda postoji idempotent $e \in R$ takav da $L = Re$ i eRe je prsten s dijeljenjem.*

Dokaz. Kako je R poluprim, postoje $x, y \in L$ takvi da $xy \neq 0$. Posebno, $Ly \neq 0$. Kako je Ly lijevi ideal od R sadržan u L iz minimalnosti od L slijedi $Ly = L$. Prema tome, postoji $e \in L$ takav da $ey = y$, odakle slijedi da $e^2 - e$ pripada skupu $J := \{z \in L \mid zy = 0\}$. Jasno, J je ponovo lijevi ideal od R sadržan u L. Kako je $x \in L \setminus J$, ovog puta zaključujemo da je $J = 0$. Posebno, $e^2 = e$. Kako je $e \in L$, imamo $Re \subseteq L$. Kako je $0 \neq e \in Re$ iz minimalnosti od L slijedi da je $L = Re$. Uzmimo sada kutni prsten eRe. Neka je $a \in R$ takav da $eae \neq 0$. Moramo pokazati da je eae invertibilan u eRe. Imamo $0 \neq Reae \subseteq Re = L$ pa je $Reae = L$. Stoga postoji $b \in R$ takav da vrijedi $beae = e$. Onda je i $(ebe)(eae) = e$. Kako je ebe nenul element u eRe, postoji $c \in R$ takav da $(ece)(ebe) = e$. Ali, lijevi inverz se poklapa s desnim pa je $eae = ece$ invertibilan u eRe s inverzom ebe.

□

Korolar 3.6.5. *Ako je A nenul konačnodimenzionalna poluprim algebra, onda postoji idempotent $e \in A$ takav da je eAe algebra s dijeljenjem.*

Dokaz. Kako je A konačnodimenzionalna, ona sadrži minimalne lijeve ideale. Npr. uzmimo bilo koji lijevi ideal najmanje dimenzije. □

Korolar 3.6.6. *Sljedeće tvrdnje su međusobno ekvivalentne za idempotent e u poluprim prstenu R:*

(i) eRe je prsten s dijeljenjem.

(ii) Re je minimalni lijevi ideal od R.

(iii) eR je minimalni desni ideal od R.

Dokaz. Kako je (i), za razliku od (ii) i (iii) simetričan uvjet, dovoljno je dokazati ekvivalenciju (i) $\Leftrightarrow$ (ii).
(ii) $\Rightarrow$ (i) slijedi iz dokaza leme 3.6.4.
(i) $\Rightarrow$ (ii) Pretpostavimo da je eRe prsten s dijeljenjem te uzmimo neki lijevi ideal I od R, takav da je $0 \neq I \subseteq Re$. Vidimo da je dovoljno pokazati da je $e \in I$. Naime, u tom slučaju je $Re \subseteq I$ pa je $I = Re$. Uzmimo neki $0 \neq u \in I$. Kako je R poluprim prsten, onda postoji $r \in R$ takav da $uru \neq 0$. Primijetimo da je $u = ue$ jer je $u \in I \subseteq Re$. Tada je $eru = erue$ nenul element u eRe. Kako je eRe prsten s dijeljenjem, postoji $v \in R$ takav da $(eve)(eru) = e$. Dakle $e \in Ru \subseteq I \Rightarrow e \in I$. □

3.7 Wedderburnovi strukturalni teoremi

Teorem 3.7.1 (Wedderburn)**.** *Neka je A nenul konačnodimenzionalna algebra. Sljedeće tvrdnje su ekvivalentne:*

(i) A je prim algebra.

(ii) A je prosta algebra.

(iii) Postoji $n \in \mathbb{N}$ i algebra s dijeljenjem D takvi da $A \cong M_n(D)$.

Dokaz.
(iii) $\Rightarrow$ (ii) slijedi direktno iz primjera 2.2.3.
(ii) $\Rightarrow$ (i) slijedi trivijalno.
(i) $\Rightarrow$ (iii) Prvo ćemo dokaz provesti uz dodatnu pretpostavku da A ima jedinicu. Dokaz provodimo indukcijom po dimenziji $d := [A : F]$.
Ako je $d = 1$, onda uzimamo $n = 1$ i $D = F$. Stoga, neka je $d > 1$. Iz korolara 3.6.5 slijedi da postoji idempotent $e \in A$ takav da je eAe algebra s dijeljenjem. Ako je $e = 1_A$, onda slijedi željeni zaključak (za $n = 1$). Pretpostavimo da je e netrivijalni idempotent. Neka je $f := 1 - e$. Primijetimo da je fAf nenul prim unitalna algebra s jedinicom f. Kako e ne pripada fAf, imamo $[fAf : F] < d$. Iz pretpostavke indukcije slijedi da je za neki $m \in \mathbb{N}$, fAf izomorfan algebri $m \times m$ matrica nad nekom algebrom s dijeljenjem. Prema tome, fAf sadrži $m \times m$ sustav matričnih jedinica e_{ij}, $i, j = 1, \ldots, m$, takve da je $e_{11}fAfe_{11} = e_{11}Ae_{11}$ algebra s dijeljenjem. Cilj nam je proširiti matrične jedinice od fAf do matričnih jedinica od A. Krećemo tako da definiramo $n := m + 1$ i $e_{nn} := e$. Onda je $\sum_{i=1}^{n} e_{ii} = f + e = 1$ te $e_{nn}e_{ij} = e_{ij}e_{nn} = 0$ za sve $i, j < n$. Preostaje naći e_{in} i e_{ni}, $i \leq n - 1$. Nađimo prvo e_{1n} i e_{n1}. Koristeći dvaput činjenicu da je A prim vidimo da je $e_{11}ae_{nn}a'e_{11} \neq 0$ za neke $a, a' \in A$. Kako je $e_{11}Ae_{11}$ algebra s dijeljenjem čija je jedinica e_{11}, postoji $a'' \in A$ takav da je

$$(e_{11}ae_{nn}a'e_{11})(e_{11}a''e_{11}) = e_{11}.$$

Ako definiramo $e_{1n} := e_{11}ae_{nn}$ i $e_{n1} := e_{nn}a'e_{11}a''e_{11}$, imamo:

$$e_{1n}e_{n1} = e_{11}.$$

Kako je $e_{n1} \in e_{nn}Ae_{11}$, imamo $e_{n1} = e_{nn}e_{n1}$ i $e_{n1} = e_{n1}e_{11} = e_{n1}e_{1n}e_{n1}$. Uspoređivanjem oba izraza dobivamo:

$$(e_{n1}e_{1n} - e_{nn})e_{n1} = 0.$$

Element $e_{n1}e_{1n} - e_{nn}$ leži u algebri s dijeljenjem $e_{nn}Ae_{nn}$. Ako bi on bio različit od nule, zadnji izraz možemo pomnožiti s lijeve strane s njegovim inverzom, što bi nas dovelo do kontradikcije $0 = e_{nn}e_{n1} = e_{n1}$. Stoga,

$$e_{n1}e_{1n} = e_{nn}.$$

Konačno, za $j = 2, \ldots, n-1$ definirajmo $e_{nj} := e_{n1}e_{1j}$ i $e_{jn} := e_{j1}e_{1n}$. Tada za sve $i, j, k = 1, \ldots, n$ vrijedi $e_{ij} = e_{i1}e_{1j}$ i $e_{1j}e_{k1} = \delta_{jk}e_{11}$. Dakle, za sve $i, j, k, l = 1, \ldots, n$ imamo

$$e_{ij}e_{kl} = e_{i1}e_{1j}e_{k1}e_{1l} = \delta_{jk}e_{i1}e_{11}e_{1l} = \delta_{jk}e_{i1}e_{1l} = \delta_{jk}e_{il}.$$

Stoga je e_{ij}, $i, j = 1, \ldots, n$, $n \times n$ sustav matričnih jedinica od A. Iz leme 3.4.3 slijedi da $A \cong M_n(D)$, gdje je $D = e_{11}Ae_{11}$.

Još preostaje dokazati implikaciju (i) $\Rightarrow$ (iii) bez pretpostavke da A ima jedinicu. Pretpostavimo da je A prim bez jedinice. Onda je $A^\sharp$ unitalna prim algebra prema lemi 3.3.2. Kako (i) povlači (iii) (a onda i (ii)) za unitalne algebre, slijedi da je $A^\sharp$ prosta. Kako je A pravi nenul ideal od $A^\sharp$, došli smo do kontradikcije. □

Napomenimo kako je algebra s dijeljenjem D iz Teorema 3.7.1 konačnodimenzionalna te vrijedi $[A : F] = n^2[D : F]$. Teorem 3.7.1 češće nalazimo u obliku koji ne uključuje prim algebre; on se obično iskazuje na sljedeći način:

$$A \text{ je prosta} \quad \Longleftrightarrow \quad A \cong M_n(D).$$

Korolar 3.7.2. *Konačnodimenzionalna algebra A je centralno prosta algebra ako i samo ako postoji $n \in \mathbb{N}$ i centralna algebra s dijeljenjem D takva da je $A \cong M_n(D)$*

Dokaz. Primjena teorema 3.7.1 i leme 2.3.2 □

Korolar 3.7.3. *Dimenzija konačnodimenzionalne centralno proste algebre je potpuni kvadrat.*

Dokaz. Imamo $[M_n(D) : F] = n^2[D : F]$. Zaključak slijedi primjenom korolara 2.6.6. □

Teorem 3.7.4 (Wedderburn)**.** *Neka je A nenul konačnodimenzionalna algebra. Tada su sljedeće tvrdnje ekvivalentne:*

(i) A je poluprim algebra.

(ii) A je poluprosta algebra.

(iii) Postoje $n_1, \ldots, n_r \in \mathbb{N}$ *i algebre s dijeljenjem* $D_1, \ldots, D_r$ *takve da je*

$$A \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r).$$

Dokaz.
(i) $\Leftrightarrow$ (ii) slijedi direktno iz korolara 3.2.10.
(iii) $\Rightarrow$ (i) slijedi trivijalno.
(i) $\Rightarrow$ (iii) Pretpostavimo da je A poluprim. Dokaz provodimo indukcijom po $d = [A : F]$. Ako je $d = 1$, onda je $A = Fa$ s $a^2 \neq 0$. Stoga je $a^2 = \lambda a$ za neko $\lambda \neq 0$, tako da je $\lambda^{-1}a$ jedinica od A. Slijedi $A \cong F$. Neka je $d > 1$. Ako je A prim, onda iz teorema 3.7.1 slijedi zaključak. Dakle, možemo pretpostaviti da postoji $0 \neq a \in A$ t.d. je $I = \{x \in A \mid aAx = 0\}$ je nenul skup. I je očito ideal od A te je stoga A poluprim algebra (napomena 3.2.9). Kako je $a \neq I$, imamo $[I : F] < d$. Iz pretpostavke indukcije slijedi da $I \cong M_{n_1}(D_1) \times \cdots \times M_{n_p}(D_p)$ za neke $n_i \in \mathbb{N}$ i algebre s dijeljenjem $D_i, i = 1, \ldots, p$. Kako svaki faktor $M_{n_i}(D_i)$ ima jedinicu tako je ima i I. Prema lemi 3.5.1 postoji ideal J od A takav da $A \cong I \times J$. Ako ponovo koristimo pretpostavku indukcije (ovaj puta za ideal J od A), zaključujemo $J \cong M_{n_{p+1}}(D_{p+1}) \times \cdots \times M_{n_r}(D_r)$ za neke $n_i \in \mathbb{N}$ i algebre s dijeljenjem $D_i, i = p+1, \ldots, r$. Time je dokaz teorema završen.

□

Napomena 3.7.5. *Iz teorema 3.7.4 posebno vidimo da su nenul konačnodimenzionalne poluprim algebre automatski unitalne.*

Bibliografija

[1] G. Berhuy, F. Oggier, *An Introduction to Central Simple Algebras and Their Applications to Wireless Communication*, American Mathematical Society, 2013.

[2] M. Brešar, *An Elementary Approach to Wedderburn's structure theory* https://arxiv.org/pdf/0902.0120.pdf

[3] M. Brešar, *Introduction to Noncommutative Algebra*, Springer, 2014.

[4] S. R. Caradus, W. E. Pfaffenberger, B. Yood, *Calkin Algebras and Algebras of Operators on Banach Spaces* Marcel Dekker, 1974.

[5] Z. Franušić, J. Šiftar, *Linearna algebra 1*, *Skripta*, PMF-Matematički odsjek, Zagreb https://web.math.pmf.unizg.hr/~fran/predavanja-LA1.pdf.

[6] I. Gogić, *Operatorske algebre*, *Skripta*, PMF-Matematički odsjek, Zagreb https://web.math.pmf.unizg.hr/~ilja/OA.pdf.

[7] T. W. Hungerford, *Algebra*, Springer, 1996.

[8] I. Kleiner, *A History of Abstract Algebra*, Birkhäuser, 2000.

[9] S. Lang, *Algebra*, Springer, 2002.

[10] L. H. Rowen, *Graduate Algebra:Noncommutative View*, American Mathematical Scoiety, 2006.

[11] B. Širola, *Algebarske strukture*, *Skripta*, PMF-Matematički odsjek, Zagreb https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf.

Sažetak

U ovom radu proučavamo neka osnovna svojstva konačnodimenzionalnih algebri s dijeljenjem. Najprije dokazujemo slavni Frobeniusov teorem, koji kaže da (do na izomorfizam) postoje točno tri realne konačnodimenzionalne algebre s dijeljenjem: Realni brojevi $\mathbb{R}$, kompleksni brojevi $\mathbb{C}$ te kvaternioni $\mathbb{H}$. Nadalje, dokazujemo Wedderburnov strukturalni teorem koji opisuje strukturu konačnodimenzionalnih poluprostih algebri; svaka takva algebra je izomorfna konačnom direktnom produktu matričnih algebri nad algebrama s dijeljenjem. Time se većina pitanja vezana uz konačnodimenzionalne poluproste algebre reducira na analogna pitanja vezana uz konačnodimenzionalne algebre s dijeljenjem.

Summary

In this thesis we explore some basic properties of finite dimensional division algebras. We first present the proof of the celebrated Frobenius theorem, which states that (up to an isomorphism) there exist precisely three real finite-dimensional division algebras: Real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$ and quaternions $\mathbb{H}$. Next, we present the proof of the Wedderburn's structure theorem which describes the structure of semisimple finite-dimensional algebras; any such algebra is isomorphic to a finite direct product of matrix algebras over some division algebras. In this way most questions concerning semisimple finite-dimensional algebras are reduced to the analogues questions for finite-dimensional division algebras.

Životopis

Petar Dević rođen je 13. srpnja 1992. godine u Zagrebu gdje je pohađao osnovnu školu i gimnaziju. 2013. godine upisuje Integrirani studij matematike i fizike - smjer nastavnički, kojim objedinjuje svoje životne interese - matematiku, fiziku te edukacijsku psihologiju i metodiku poučavanja.